IB 04/50962

Europäisches Patentamt | European Patent Office | Office européen des brevets

MAILED 24 JUN 2004

WIPO PCT

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03101971.4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03101971.4
Demande no:

Anmeldetag:
Date of filing: 02.07.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH
Steindamm 94
20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Verfahren zur Eingabe eines Sicherungscodes für ein Netzwerkgerät

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G10L15/26

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

BESCHREIBUNG

Verfahren zur Eingabe eines Sicherungscodes für ein Netzwerkgerät

Die Erfindung betrifft ein Verfahren zur Eingabe eines Sicherungscodes in ein Datenverarbeitungsgerät, welches insbesondere in ein Netzwerk eingebunden werden kann. Ferner betrifft sie ein entsprechend eingerichtetes Datenverarbeitungsgerät sowie ein Netzwerk mit mindestens einem solchen Datenverarbeitungsgerät.

Bei datenverarbeitenden elektronischen Geräten besteht eine zunehmende Tendenz zur drahtlosen Vernetzung der Geräte untereinander. Eine drahtlose Kommunikation ist indes leichter anfällig für ein unautorisiertes Abhören, sodass vertrauliche Daten oder digitale Musik- oder Videodaten gestohlen werden können. Um vor diesem Hintergrund beispielsweise drahtlose digitale Heimnetzwerke zu schützen, müssen die Netzwerkgeräte (Computer, Videorecorder, TV-Geräte, Lautsprecher etc.) kryptographische Mechanismen zur Verschlüsselung des Datenverkehrs und zur Authentifizierung der Zugangsberechtigten enthalten. Alle derartigen Mechanismen beruhen auf der Existenz eines geheimgehaltenen Sicherungscodes, welcher allen Kommunikationspunkten bekannt ist, nicht jedoch einem potentiellen Abhörer. Der geheime Sicherungscode kann dann bei einer Kommunikation zwischen den Stationen als Schlüssel (pre-shared key) für Algorithmen der Kryptographie oder Authentifizierung verwendet werden.

Die Eingabe eines geheimgehaltenen Sicherungscodes kann beispielsweise bei der Produktion der an einem Netzwerk beteiligten Geräte geschehen. Dies hat jedoch den Nachteil, dass Geräte verschiedener Hersteller in der Regel nicht miteinander kombiniert werden können. Weiterhin ist es bekannt, Sicherungscodes von Hand an den Geräten einzugeben, was allerdings voraussetzt, dass die Geräte mit einer entsprechenden Tastatur oder dergleichen ausgerüstet sind. Ferner ist ein solches Eingabeverfahren verhältnismäßig kompliziert und

umständlich, was insbesondere in Hinblick auf den möglichst breiten Nutzerkreis digitaler Heimnetzwerke von Nachteil ist.

Aus der WO 02/078249 A1 ist ein Verfahren bekannt, bei welchem aus biometrischen Informationen eines Benutzers wie beispielsweise der Stimme, der Handschrift oder einem Fingerabdruck ein geheimer Schlüssel für ein Netzwerk erzeugt wird. Entsprechend der Zielrichtung des Verfahrens ist der Schlüssel dabei individuell für jeden Benutzer, sodass zwei unterschiedliche Benutzer nicht denselben Schlüssel eingeben bzw. verwenden können.

Vor diesem Hintergrund war es eine Aufgabe der vorliegenden Erfindung, Mittel zur möglichst einfachen, nutzerfreundlichen Eingabe eines Sicherungscodes in ein Datenverarbeitungsgerät bereitzustellen.

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 1, durch ein Datenverarbeitungsgerät mit den Merkmalen des Anspruchs 6 sowie durch ein Netzwerk mit den Merkmalen des Anspruchs 10 gelöst. Vorteilhafte Ausgestaltungen sind in den Unteransprüchen enthalten.

Das erfindungsgemäße Verfahren dient der Eingabe eines Sicherungscodes in ein Datenverarbeitungsgerät, welches diesen Code zur Ausführung seiner Funktion benötigt. Der Sicherungscode kann beispielsweise ein Passwort sein, welches den Benutzer als zur Bedienung des Datenverarbeitungsgerätes berechtigt ausweist (authentifiziert). Ferner kann es sich bei dem Sicherungscode auch um einen kryptographischen Schlüssel handeln, welcher von den Teilnehmern eines Netzwerkes zur Sicherung ihrer Kommunikation untereinander verwendet wird. Das Verfahren umfasst die folgenden Schritte:

a) Aufzeichnung der Audiodaten, welche entstehen, wenn von einem Benutzer eine Folge von Phonemen vorgesprochen wird. Bei Phonemen handelt es sich definitionsgemäß um die

kleinsten lautlichen Segmente einer Sprache mit bedeutungsunterscheidender Funktion. Die Audiodaten können als Rohdaten insbesondere durch mit einem Mikrofon gemessene Druckschwankungen (Schall) repräsentiert werden.

b) Ableitung eines auf der Folge der Phoneme basierenden Sicherungscodes aus den aufgezeichneten Audiodaten. Bevorzugte Verfahren für die Durchführung einer derartigen Ableitung werden in Verbindung mit den speziellen Ausgestaltungen des Verfahrens sowie bei der Figurenbeschreibung näher erläutert.

Das Verfahren hat den Vorteil, dass es von einem Benutzer in besonders einfacher Weise und ohne vertiefte Kenntnisse hinsichtlich der Bedienung des Datenverarbeitungsgerätes ausgeführt werden kann, da der Benutzer lediglich eine Folge von Phonemen vorzusprechen braucht. Die Folge von Phonemen wird dabei typischerweise durch ein Wort oder eine längere Wortfolge (Phrase, Satz) erzeugt, sodass der Benutzer sich diese Folge leicht merken und sie ohne Probleme aussprechen kann. Da der abgeleitete Sicherungscode auf der vorgesprochenen Folge der Phoneme basiert, ist gewährleistet, dass das Verfahren unabhängig von der Person des Benutzers arbeitet. Wichtig ist nur die Folge der Phoneme, dass heißt das Passwort oder die Passphrase.

Gemäß einer bevorzugten Ausgestaltung des Verfahrens werden die aufgezeichneten Audiodaten in eine geschätzte Folge von Phonemen unterteilt und diese geschätzten Phoneme jeweils einer Phonemgruppe aus einer vorgegebenen Phonemgruppeneinteilung zugeordnet. Die so entstehende Folge von Phonemgruppen beschreibt dann den gesuchten Sicherungscode. Beispielsweise können in diesem Zusammenhang die Phonemgruppen durch eine Reihe von Ziffern 1, 2, ... N nummeriert werden, sodass die Folge von Phonemgruppen einer Ziffernfolge entspricht, die sich z.B. binär repräsentieren lässt.

Bei dem vorstehend beschriebenen Vorgehen wird vorzugsweise ein Qualitätsmaß dafür berechnet, wie sicher die vorgenommene Zuordnung der Audiodaten zu den Phonemgruppen ist. Das Qualitätsmaß kann dabei insbesondere die Sicherheit der Unterteilung der Audiodaten in eine geschätzte Folge von Phonemen und/oder die Zuordnung der geschätzten Phoneme zu den Phonemgruppen bewerten. Durch ein solches Qualitätsmaß lässt sich beurteilen, ob der berechnete Sicherungscode mit ausreichend hoher Wahrscheinlichkeit der vom Benutzer gewünschten Eingabe entspricht oder nicht. Falls das Qualitätsmaß zu gering ist, kann der Benutzer dabei zu einer erneuten Eingabe aufgefordert werden.

Gemäß einer anderen Weiterbildung des Verfahrens werden in den Audiodaten enthaltene biometrische Charakteristika der Stimme des Benutzers zur Authentifizierung des Benutzers verwendet. Dass heißt, dass anhand der genannten Charakteristika entschieden wird, ob der vorsprechende Benutzer überhaupt zur Bedienung des Datenverarbeitungsgerätes berechtigt ist oder nicht. Nur dann, wenn der Benutzer zur Bedienung autorisiert ist, wird die von ihm vorgesprochene Folge von Phonemen (Passwort, Passphrase) zur Ableitung eines Sicherungscodes verwendet.

Die Erfindung betrifft ferner ein Datenverarbeitungsgerät, welches zur Ausübung seiner Funktion die Vorgabe eines Sicherungscodes benötigt. Das Datenverarbeitungsgerät kann zum Beispiel ein Gerät für ein digitales Heimnetzwerk wie etwa ein CD-Spieler, ein Satellitenempfänger, ein TV-Gerät oder dergleichen sein. Das Datenverarbeitungsgerät enthält die folgenden Komponenten:

a) Eine Sprachaufzeichnungseinheit zur Aufzeichnung der entstehenden Audiodaten, wenn von einem Benutzer eine Folge von Phonemen vorgesprochen wird.

b) Eine mit der Sprachaufzeichnungseinheit gekoppelte Sprachanalyseeinheit zur Ableitung eines auf der Folge von Phonemen basierenden Sicherungscodes aus den aufgezeichneten Audiodaten.

Das Datenverarbeitungsgerät implementiert das oben erläuterte Verfahren. Für die detailliertere Beschreibung seiner Funktion, seiner Vorteile und der möglichen Varianten des Datenverarbeitungsgerätes wird daher auf die obige Beschreibung Bezug genommen.

Das Datenverarbeitungsgerät kann insbesondere eine Anzeige (Display, Leuchtdiode, Lautsprecher etc.) enthalten und dazu eingerichtet sein, den Benutzer mit Hilfe der Anzeige auf den Fall hinzuweisen, dass aufgezeichnete Audiodaten nicht zur Ableitung eines Sicherungscodes verwendet werden können. Zum Beispiel kann die Qualität der Audiodaten zu schlecht sein, um hieraus mit ausreichender Zuverlässigkeit einen Sicherungscode abzuleiten.

Des Weiteren kann das Datenverarbeitungsgerät eine Kommunikationsschnittstelle für eine drahtlose Kommunikation mit einem Netzwerk enthalten. In diesem Falle kann das Gerät in ein solches Netzwerk eingebunden werden und der Sicherungscode insbesondere für eine Verschlüsselung der Kommunikation im Netzwerk verwendet werden.

Die Erfindung betrifft ferner ein Netzwerk aus miteinander kommunizierenden Geräten, wobei insbesondere mindestens ein Subnetzwerk vorhanden ist, welches mit dem Rest des Netzwerkes über eine oder mehrere drahtlose Verbindungen gekoppelt ist, wobei vorzugsweise keine weiteren drahtgebundenen Verbindungen bestehen. In diesem Subnetzwerk soll dabei mindestens ein Datenverarbeitungsgerät der oben beschriebenen Art vorhanden sein, welches die Eingabe eines Sicherungscodes durch Vorsprechen eines Passworts oder einer Passphrase durch einen Benutzer ermöglicht. Insbesondere können natürlich alle am Netzwerk beteiligten Geräte von dieser Art sein, sodass sämtliche für eine drahtlose Kommunikation benötigten Verschlüsselungscodes auf dieselbe einfache Weise per Sprache vorgegeben werden können.

Im Folgenden wird die Erfindung mit Hilfe der Figur beispielhaft erläutert. Die einzige Figur zeigt ein drahtloses Heimnetzwerk mit einem erfindungsgemäßen Datenverarbeitungsgerät zur Spracheingabe eines Sicherungscodes.

Das in der Figur schematisch dargestellte Heimnetzwerk enthält verschiedene Geräte wie beispielsweise einen Audio/Videorecorder 9c, Stereolautsprecher 9a, 9b und ein TV-Gerät 9d, welche untereinander drahtlos kommunizieren. Um die dabei ausgetauschten Daten gegen ein missbräuchliches Abhören zu schützen, wird die Kommunikation mit Hilfe eines geheimen, nur den Netzteilnehmern bekannten Sicherungscodes verschlüsselt.

Wenn ein neues Datenverarbeitungsgerät 2 in das Netzwerk 10 eingebracht werden soll, muss ihm der dort verwendete Sicherungscode eingegeben werden. Das Gerät 2 enthält erfindungsgemäß zu diesem Zweck die nachfolgend erläuterten Komponenten:

- ein Mikrofon 6 mit einer daran angeschlossenen Audioschaltung 3, die gemeinsam eine Sprachaufzeichnungseinheit für die Aufzeichnung akustischer Informationen in Form von digitalisierten Audiodaten (zum Beispiel *.wav Dateien) bilden;
- eine mit der Sprachaufzeichnungseinheit gekoppelte Sprachanalyseeinheit 4, welche die aufgezeichneten Audiodaten in der nachfolgend noch zu beschreibenden Weise analysiert, um hieraus den gesuchten Sicherungscode abzuleiten;
- ein Kernmodul 5, welches die eigentliche Funktion des Gerätes 2 ausführt und hierfür den Sicherungscode benötigt;
- eine Kommunikationsschnittstelle 8 zur drahtlosen Kommunikation mit anderen Teilnehmern eines Netzwerkes;
- eine Anzeigeeinheit 7, zum Beispiel ein LCD-Display, welche insbesondere von der Sprachanalyseeinheit 4 angesteuert werden kann.

Zur Eingabe eines Sicherungscodes in das beschriebene Gerät 2 wird dieses zunächst von einem Benutzer 1 in einen Schlüssel-Empfangsmodus geschaltet. Der Benutzer 1 spricht dann ein Passwort oder eine längere Passphrase in das Mikrofon 6, wobei die zugehörigen Audiodaten aufgezeichnet werden. Das System überprüft dabei unmittelbar, ob die gesprochene Information lang genug für die Erzeugung eines Sicherungscodes ist. Gegebenenfalls wird der Benutzer 1 über die Anzeige 7 darauf hingewiesen, dass er ein andere (längere) Wortfolge vorsprechen muss.

In der Sprachanalyseeinheit 4 werden die Audiodaten mit bekannten Verfahren (vgl. zum Beispiel US 4 924 518) in eine zugehörige Folge von (geschätzten) Phonemen konvertiert. Diese Phoneme werden dann jeweils einer Phonemgruppe zugeordnet. Die Phonemgruppen umfassen dabei einander ähnliche Phoneme, wobei die Phonemgruppeneinteilung vorgegeben ist und zum Beispiel bei der Herstellung des Gerätes 2 in dessen Hardware implementiert wird. Die Phonemgruppen können durch Ziffern 1, 2, ... N indiziert werden, sodass die Folge der Phonemgruppen in eine Folge solcher Ziffern übersetzt werden kann. Diese Zahlenfolge kann wiederum in eine Bitfolge umgewandelt werden, welche dann den gesuchten Sicherungscode repräsentiert.

Vorzugsweise nutzt das Gerät 2 noch die Qualität der aufgezeichneten Audiodaten zur Abschätzung einer Fehlerwahrscheinlichkeit dafür, dass eine falsche Zuordnung von ein oder mehreren Phonemgruppen erfolgt ist. Wenn die so abgeschätzte Fehlerwahrscheinlichkeit höher als eine vorgegebene Schwelle ist, wird der Benutzer 1 über die Anzeige 7 aufgefordert, die Aufzeichnung der Audiodaten durch erneutes Vorsprechen der Passphrase zu wiederholen. Im Übrigen kann die Richtigkeit des Sicherungscodes natürlich auch durch eine standardmäßig verlangte Wiederholung der Passphrase verifiziert werden.

Für die Konfiguration des im Netzwerk 10 neuen Gerätes 2 muss der Benutzer 1 somit nur während des Schlüssel-Empfangsmodus eine Passphrase vorsprechen und den Schlüssel-

Empfangsmodus anschließend wieder abstellen. Das Gerät 2 leitet sich aus der Passphrase automatisch den Sicherungscode ab und überträgt ihn über eine interne Schnittstelle an die entsprechende Treibersoftware, welche die drahtlose Schnittstelle 8 des Gerätes 2 kontrolliert. Der Sicherungscode kann dann von dem Gerät 2 bei der Ausführung von Algorithmen der Kryptographie und Authentifizierung verwendet werden, um die Kommunikation mit anderen Stationen des Heimnetzwerkes 10 zu schützen und zu überprüfen. Da der Sicherungscode von allen Geräten 2, 9a-9d des Heimnetzwerkes verwendet wird, erfolgt die Kontrolle der Zugangsberechtigung zum Netzwerk 10 über die Kenntnis des gemeinsamen Schlüssels.

Vorzugsweise ist jedes eine Schnittstelle zur drahtlosen Kommunikation aufweisende Gerät des Heimnetzwerkes 10 in der beschriebenen Weise wie das Gerät 2 ausgestaltet. Bei der Einrichtung des Netzwerkes 10 kann dann ein allen Geräten bekannter Sicherungscode von einem Benutzer in einfacher Weise durch Vorsprechen einer Passphrase bei jedem Gerät (oder, falls praktikabel, durch einmaliges Vorsprechen in mehrere Gerätemikrofone gleichzeitig) vorgegeben werden.

BEZUGSZEICHENLISTE

	1	Benutzer
	2	Gerät
5	3	Audioschaltung
	4	Sprachanalyseeinheit
	5	Kernmodul
	6	Mikrofon
	7	Anzeige
10	8	drahtlose Schnittstelle
	9a-d	Netzwerkgeräte
	10	Netzwerk

PATENTANSPRÜCHE

1. Verfahren zur Eingabe eines Sicherungscodes in ein Datenverarbeitungsgerät (2), umfassend die Schritte

   a) Aufzeichnung der entstehenden Audiodaten, wenn von einem Benutzer (1) eine Folge von Phonemen vorgesprochen wird;

   b) Ableitung eines auf der Folge der Phoneme basierenden Sicherungscodes aus den aufgezeichneten Audiodaten.

2. Verfahren nach Anspruch 1,
   dadurch gekennzeichnet,
   dass der Sicherungscode einen kryptographischen Schlüssel für eine gesicherte Kommunikation in einem Netzwerk (10) darstellt.

3. Verfahren nach Anspruch 1 oder 2,
   dadurch gekennzeichnet,
   dass die Audiodaten in eine geschätzte Folge von Phonemen unterteilt und diese Phoneme jeweils einer Phonemgruppe aus einer vorgegebenen Phonemgruppeneinteilung zugeordnet werden, wobei die so entstehende Folge von Phonemgruppen den gesuchten Sicherungscode beschreibt.

4. Verfahren nach Anspruch 3,
   dadurch gekennzeichnet,
   dass ein Qualitätsmaß dafür berechnet wird, wie sicher die Zuordnung der Audiodaten zu den Phonemgruppen ist.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
dass in den Audiodaten enthaltene biometrische Charakteristika zur Authentifizierung eines Benutzers (1) verwendet werden.

6. Datenverarbeitungsgerät (2), welches zur Ausübung seiner Funktion die Vorgabe eines Sicherungscodes benötigt, enthaltend
   a) eine Sprachaufzeichnungseinheit (3, 6) zur Aufzeichnung der entstehenden Audiodaten, wenn von einem Benutzer (1) eine Folge von Phonemen vorgesprochen wird;
   b) eine mit der Sprachaufzeichnungseinheit (3, 6) gekoppelte Sprachanalyseeinheit (4) zur Ableitung eines auf der Folge der Phoneme basierenden Sicherungscodes aus den aufgezeichneten Audiodaten.

7. Datenverarbeitungsgerät nach Anspruch 6,
dadurch gekennzeichnet,
dass es dazu eingerichtet ist, ein Verfahren nach einem der Ansprüche 1 bis 5 auszuführen.

8. Datenverarbeitungsgerät nach Anspruch 6 oder 7,
dadurch gekennzeichnet,
dass es dazu eingerichtet ist, den Benutzer (1) über eine Anzeige (7) darauf hinzuweisen, wenn aufgezeichnete Audiodaten nicht zur Ableitung eines Sicherungscodes verwendet werden können.

9. Datenverarbeitungsgerät nach mindestens einem der Ansprüche 6 bis 8,
dadurch gekennzeichnet,

dass es eine Kommunikationsschnittstelle (8) für eine drahtlose Kommunikation mit einem Netzwerk (10) enthält.

10. Netzwerk (10) aus miteinander kommunizierenden Geräten (2, 9a-9d), wobei in einem über mindestens eine drahtlose Verbindung angekoppelten Subnetzwerk ein Datenverarbeitungsgerät (2) nach einem der Ansprüche 6 bis 9 vorhanden ist.

ZUSAMMENFASSUNG

Verfahren zur Eingabe eines Sicherungscodes für ein Netzwerkgerät

Die Erfindung betrifft ein Verfahren zur Eingabe eines Sicherungscodes wie insbesondere eines gemeinsamen Schlüssels zur Sicherung der Kommunikation in einem drahtlosen Netzwerk (10) in ein Datenverarbeitungsgerät (2). Die von einem Benutzer (1) vorgesprochene Passphrase wird dabei von einer Sprachaufzeichnungseinheit (3, 6) in Form von Audiodaten aufgezeichnet. Die Audiodaten werden von einer Sprachanalyseeinheit (4) in eine Folge von Phonemen bzw. Phonemgruppen unterteilt, welche den gesuchten Sicherungscode repräsentiert.

Fig. 1